



■ Di **Simone Zanardi**

PMI LA RETE IDEALE



I piccoli e medi uffici non possono più fare a meno di una struttura informatica articolata e versatile. Ecco alcuni consigli per installare un network allo stato dell'arte.

Il network aziendale è la spina dorsale della struttura informatica, e quindi produttiva, degli uffici, qualsiasi sia la loro dimensione. Anche le piccole e medie realtà non possono fare a meno di una rete che si adatti perfettamente alle esigenze del personale e dei processi aziendali, pena una drastica riduzione dell'efficienza e un conseguente rialzo dei costi. Nel corso degli ultimi anni queste esigenze sono cambiate radicalmente: dopo una fase in cui la parola d'ordine è stata "convergenza", con particolari riferimenti a telefonia e videosorveglianza, oggi i paradigmi chiave sono quelli della mobilità, del cloud e della condivisione. Sono cambiati i dispositivi terminali, con tablet e smartphone che non si limitano ad affiancare il computer, ma puntano a sostituirlo in numerose attività, mentre le applicazioni stanno sempre più tramutandosi in servizi.

È mutato anche il modo in cui si condividono le informazioni e si collabora, grazie ai nuovi servizi di storage online e alle piattaforme di sharing dedicate al mondo aziendale. La rete deve adeguarsi a queste nuove modalità: sia che dobbiate installare un nuovo network sia che dobbiate rinnovare la struttura esistente, ecco alcuni suggerimenti per far rendere al meglio il vostro sistema informatico.

Prima di analizzare i singoli aspetti di un network aziendale di piccole dimensioni, è importante evidenziare alcune considerazioni di carattere generale. In primo luogo, quando si progetta una nuova installazione, è bene trovare il giusto bilanciamento tra esigenze presenti e possibili evoluzioni necessarie nel futuro. L'approccio ottimale è quello della scalabilità, che a sua volta richiede una visione modulare che permetta di aggiungere e aggiornare elementi della rete senza dover riconfigurare ogni volta l'intera

struttura. Da questo punto di vista è ad esempio importante investire sul cablaggio strutturato, soprattutto se i locali dell'ufficio non sono predisposti con pavimenti flottanti, torrette o altre strutture che facilitino l'accesso ai cavi di rete. Come vedremo nelle prossime pagine, infatti, in ambito professionale i collegamenti via cavo sono pressoché imprescindibili per garantire le massime prestazioni e affidabilità alla Lan (Local Area Network).

Per quanto concerne gli apparati, è importante investire su dispositivi in linea con la propria categoria di utilizzo, evitando di farsi prendere la mano dalle esigenze di risparmio da un lato e da servizi e prodotti sovradimensionati dall'altro. In ambito di piccole e medie aziende è infatti molto facile pensare ad esempio che un dispositivo consumer o Soho possa fornire le medesime prestazioni o affidabilità di un modello professionale, magari perché le specifiche principali sono le medesime.

D'altro canto, è bene non farsi inganare dalle promesse di potenza o funzionalità di alcuni prodotti dedicati all'ambito enterprise che spesso non solo forniscono servizi sovradimensionati, ma complicano installazione, configurazione e gestione dell'intero sistema di networking laddove il personale It sia assente o limitato.

Nelle prossime pagine ci concentreremo su alcuni aspetti peculiari di una moderna rete informatica per il piccolo e medio ufficio, a partire dalla struttura base che fornisce la connettività, passando per la gestione dei collegamenti senza fili e dei dispositivi mobili di nuova generazione, sino ad arrivare ai metodi migliori per integrare la rete con i servizi cloud e per renderla più affidabile. Per ogni punto oltre a offrire una panoramica generale indicheremo alcuni *tip* rapidi che possono essere utili nella ricerca dei dispositivi, dei software e dei servizi più adatti alle vostre esigenze.

«I dispositivi consumer non forniscono le stesse prestazioni e affidabilità dei modelli dedicati all'utenza professionale, anche entry-level.»



ACCESSO A INTERNET

La tecnologia di accesso a banda larga più diffusa in Italia, anche in ambito di piccole e medie aziende, è senza dubbio la Adsl, che sfrutta il doppino telefonico per portare all'utente finale velocità massime teoriche nell'ordine dei 10-20 Megabit al secondo. Come lo stesso acronimo indica, le *Asymmetric Digital Subscriber Line* sono connessioni di tipo asimmetrico, ovvero offrono velocità maggiori nella direzione di downlink (trasferimenti da Internet verso la rete locale) rispetto a quelle di uplink, ovvero per i trasferimenti nella direzione opposta.

Le linee asimmetriche di questo tipo sono più che adeguate per applicazioni come la navigazione su pagine Web o il download di software e documenti, ma con la crescente diffusione dei servizi *cloud-based* anche le prestazioni in uplink stanno divenendo sempre più importanti. Si pensi ad esempio a un gruppo di lavoro che condivide i documenti su di una piattaforma di storage online come Dropbox.

Da questo punto di vista, se tra le offerte di connettività a cui potete accedere vi sono pacchetti basati su tecnologie più efficienti in uplink come la fibra ottica o Hdsl il nostro consiglio è di esaminare dapprima queste soluzioni. Se l'Adsl è l'unica opzione disponibile, non fermatevi alla tanto pubblicizzata velocità di punta in downlink, ma controllate anche le performance nominali in uplink e verificate che possano soddisfare le vostre esigenze.

Altro parametro da controllare con attenzione è la velocità minima garantita: le connessioni Adsl si basano su risorse

quanta banda il provider è in grado di mettere a disposizione nel caso pessimo, e quindi la soglia sotto la quale non si dovrebbe mai scendere.

Oltre che alla velocità, è bene badare all'affidabilità dell'accesso a Internet: per garantire continuità di servizio in caso di problematiche è possibile sottoscrivere un secondo contratto di connessione, che subentri al principale quando necessario. In questo ambito il nostro consiglio è quello di appoggiarsi a una tecnologia differente (una doppia connessione Adsl sarebbe inutile in caso di interruzione della rete telefonica), rivolgendosi ad esempio alle connessioni tramite rete cellulare o provider wireless. Se lo scopo della seconda linea è solo quello di subentrare in caso di emergenza, ci si può indirizzare verso un contratto che preveda un pagamento a traffico o a durata della connessione per minimizzare i costi.

Molti provider al momento della sottoscrizione del contratto di connessione offrono un modem/router in comodato d'uso, già configurato per l'accesso alla Rete. In ambito aziendale è quasi sempre consigliabile sostituirlo o affiancarlo con un router di proprietà, sia per poter scegliere un dispositivo con le caratteristiche tecniche più indicate alle specifiche esigenze dell'azienda sia per le maggiori possibilità di personalizzazione. In questo senso le realtà di medie e piccole dimensioni possono trovare spesso soluzioni ideali nei router che integrano al loro interno firewall e sistemi di Utm (*Unified Threat Management*).

I router professionali con doppia Wan possono gestire più canali di accesso verso Internet.

Cinque tip



1 Asimmetrico ma non troppo

Come vedremo nelle prossime pagine, il cloud sarà sempre più pervasivo in ambito aziendale nei prossimi mesi. Per poter interagire al meglio con le strutture di storage e servizi online, è importante disporre di velocità non solo in downlink, ma anche nel senso opposto (uplink, ovvero caricamento dei file dalla Lan a Internet).

2 Minimo garantito

Un altro parametro da controllare al momento di scegliere il proprio provider di accesso è la velocità minima garantita, al di là della massima nominale. In questo modo vi assicurerete che anche nei momenti di maggior traffico le prestazioni del vostro collegamento non scenderanno sotto una data soglia.

3 Una linea di backup

In casi di guasti o problematiche sulla linea di accesso principale, può essere utile disporre di un canale secondario di connessione. In questo caso è bene non affidarsi alla medesima tecnologia (es. Adsl), ma rivolgersi a un canale alternativo (Wisp, o accesso da rete cellulare).

4 Router di proprietà

I router forniti dal provider sono spesso limitati e poco configurabili: sostituiteli con un dispositivo di proprietà che si adatti alle vostre esigenze. Potete anche installarlo in cascata al dispositivo datovi dall'Isp, sfruttando quest'ultimo solo come gateway.

5 Sicurezza periferica

Nelle reti di grandi dimensioni è imprescindibile disporre di un firewall dedicato alla protezione periferica del network, ma per un piccolo e medio ufficio può essere sufficiente un router evoluto con caratteristiche di sicurezza avanzate (Unified Threat Management, Content filtering e Antivirus, per esempio).



LA STRUTTURA

La struttura di una rete aziendale di piccole e medie dimensioni vede la tecnologia di cablaggio su rame come soluzione da privilegiare: l'alternativa in fibra ottica è infatti raramente necessaria per le piccole realtà (è indicata soprattutto per la copertura di distanze superiori ai 100 metri e per i collegamenti interdipartimentali), mentre il wireless, di cui come vedremo non si può comunque fare a meno, non offre le stesse prestazioni e affidabilità.

La classica struttura di rete prevede un centro-stella, tipicamente collocato nella sala server o nella zona dove è installato il router per l'accesso a Internet. Nel centro stella è situato lo switch da cui si diramano i vari cablaggi che raggiungono le postazioni di lavoro. I cavi Ethernet sono di tipo *twisted pair* (a coppie incrociate); si tratta di cavi del diametro di circa 4 mm che si suddividono in categorie, indicanti la qualità costruttiva e la banda passante che sono in grado di supportare. Considerate esclusivamente cablaggi Cat5e (sino a 100 MHz) e Cat6 (250 MHz) o superiori: i primi possono gestire le connessioni Gigabit Ethernet, seppur giungendo al limite estremo delle proprie capacità, i secondi garantiscono ulteriore affidabilità in caso di collegamenti a 1.000 Mbps e 10 Gbps.

Nella scelta dello switch, il fattore essenziale da considerare per la Pmi è la velocità e numero delle porte. Il numero delle porte è chiaramente proporzionale ai punti rete da attivare nell'ufficio; in quest'ottica è bene non essere avari, dotandosi di porte libere in previsione di un'eventuale espansione della rete. Anche se la vostra rete non prevede applicazioni VoIP (*Voice Over IP*), se state pianificando il network da zero prevedete due porte di accesso per ogni scrivania.

Gli switch oggi in commercio offrono sino a 48 porte su singola unità, mentre per esigenze di maggior connettività è possibile ricorrere ad apparati con opzione stack (due o più switch possono essere collegati in pila attraverso un cavo di backbone ad altissima velocità). Lo standard minimo di velocità deve essere il Gigabit Ethernet, ma se utilizzate applicazioni intensive dal punto di vista del trasferimento dati può tornare utile un canale di comunicazione ancora più performante, perlomeno verso il server centrale o il Nas.

Se il server le supporta, potete utilizzare due porte Gigabit Ethernet in aggregazione di banda, o ancora meglio una connessione a 10 Gbps su rame. Sul mercato potete trovare switch a 1 Gbps che però includono una o due porte 10 Gigabit Ethernet per questo scopo.

Oltre che dalla velocità delle porte, uno switch è caratterizzato dalle sue funzioni di gestione del traffico. In questo ambito si distinguono switch di secondo e di terzo livello, gestiti o non gestiti. Gli switch di terzo livello offrono funzioni simili a quelle di un router, agendo sui pacchetti di traffico in transito a livello di protocollo IP. Spesso sono sovradimensionati per reti di piccola entità. Molto più utile è uno switch gestito, ovvero un apparato sul quale si può intervenire per configurare i parametri essenziali di funzionamento. Uno switch gestito permette ad esempio di definire delle reti locali virtuali (Vlan), in modo da segmentare il traffico e creare direttrici dedicate per le comunicazioni più sensibili.

Una citazione finale per le Powerline: la tecnologia che sfrutta i cablaggi elettrici per trasmettere dati tra due postazioni è indicata soprattutto per l'ambito consumer, ma in casi particolari (cablaggio di rete impossibile e Wi-Fi inefficiente, può tornare utile anche nel business.

Cinque tip

1 Più porte per tutti
Per ogni postazione di lavoro, approntate perlomeno due porte di rete: per quanto non sia complicato moltiplicare il numero di interfacce tramite uno switch secondario, è sempre bene massimizzare la connettività per non essere poi costretti a re-intervenire sul cablaggio.

2 Il Wi-Fi solo dove serve
Come vedremo tra poco, una struttura di accesso wireless è ormai indispensabile per qualsiasi rete. Per prestazioni ed affidabilità i Wi-Fi non è però paragonabile al cavo. Dove è possibile, ricorrere quindi al cablaggio Gigabit Ethernet.

3 Uno switch adeguato
Lo switch rappresenta il centro della rete: è bene sacrificare parte del budget per acquistare un dispositivo in grado di supportare al meglio le connessioni, anche in ottica di espansione futura. Gigabit Ethernet per tutti, qualche porta in più rispetto all'indispensabile e, in caso di reti complesse, switch gestiti e configurabili.

4 Oltre il gigabit
Nelle realtà di piccole dimensioni (anche fisiche) la tecnologia Gigabit Ethernet è più che adeguata. Il collegamento dallo switch a un server centrale può però trarre beneficio da velocità ancora superiori. In questi casi ci si può rivolgere a uno switch con una o due porte 10 Gbps integrate.

5 Powerline: perché no?
Pur ribadendo ancora una volta la supremazia del cablaggio tradizionale in ambito professionale, in casi particolari (edifici storici, dove gli interventi di posa sono di fatto impossibili) gli apparati Powerline, che sfruttano la rete elettrica per le comunicazioni dati, possono essere indicati.



Molti switch Gigabit Ethernet sono dotati di due o più porte a 10 Gbps per l'aggancio di server o link in fibra.

Cinque tip

1 Sicurezza al top

Per massimizzare la sicurezza delle connessioni Wi-Fi, utilizzate autenticazioni basate su server Radius/802.1x, in questo modo ogni utente disporrà di proprie credenziali, rinnovabili o rimovibili in caso di necessità senza dover reimpostare tutti gli altri account.

2 Differenziare gli accessi

Molti sistemi wireless professionali permettono di definire più reti wireless virtuali. Segmentando i diritti di accesso si possono così creare collegamenti per i clienti e i fornitori che si presentano in ufficio e devono utilizzare Internet senza poter accedere ai server aziendali.

3 Access point multipli

Un singolo punto di accesso è probabilmente sufficiente a soddisfare le esigenze di un piccolo e medio ufficio in termini di copertura, ma con il moltiplicarsi dei dispositivi collegati in modalità senza fili (anche due o più per ogni utente), potrebbe essere utile bilanciare il carico tra più stazioni.

4 Doppia banda contro le interferenze

Molti access point 802.11n o 802.11ac supportano sia le trasmissioni a 2,4 GHz sia quelle a 5 GHz. Queste ultime sono meno soggette alle interferenze provenienti da altri dispositivi cordless. Se il vostro ufficio è teatro di "inquinamento" a 2,4 GHz, potete rivolgervi ad apparati dual radio.

5 Aderenza agli standard

È generalmente buona pratica affidare la propria struttura wireless a dispositivi di un unico vendor, ma in caso contrario verificate l'aderenza agli standard 802.11, possibilmente acquistando apparati dotati di certificazione della Wi-Fi Alliance.



Gli access point professionali integrano funzioni ideali per le Pmi come la gestione di profili di accesso multipli.

SENZA FILI, MAI SENZA

Abbiamo detto della supremazia del cavo sul Wi-Fi dal punto di vista delle prestazioni e dell'affidabilità. Ciò non toglie che una struttura wireless sia altrettanto imprescindibile per un'azienda moderna, anche di piccole dimensioni. Il Wi-Fi è innanzitutto l'unica tecnologia che permette l'accesso alla rete da parte di smartphone e tablet, dispositivi sempre più essenziali in ogni realtà produttiva. Inoltre, il wireless è spesso soluzione ideale per gli ambienti dove la posa dei cavi sia realmente impraticabile (edifici storici). Da ultimo, una buona rete Wi-Fi semplifica l'interazione con clienti, fornitori e collaboratori, oltre che con i normali visitatori.

Per le realtà di dimensioni più limitate, la rete wireless può essere gestita da un singolo access point. In questi casi è però importante rivolgersi a un apparato professionale, che offra alcune funzioni evolute tra cui la gestione degli account di accesso. Nelle installazioni wireless professionali, infatti, difficilmente ci si può accontentare di un sistema a password condivisa.

Il sistema di accesso deve essere invece organizzato in account personali. La tecnologia Wi-Fi prevede in questi casi l'interazione con un server di autenticazione già presente in rete a cui interfacciarsi tramite il protocollo 802.1x. In assenza di questo servizio, molti access point professionali possono gestire un database interno di utenti locali.

Altra caratteristica diffusa negli access point professionali è la possibilità di definire Ssid virtuali multipli: in questo modo a partire da una sola stazione base si creano di fatto due o più reti wireless, ciascuna dotata di proprie caratteristiche di sicurezza e policy di

accesso. Un Ssid può essere utilizzato ad esempio per definire una rete ospite che offra accesso a Internet ma non ai server locali.

Le reti più articolate possono appoggiarsi a un sistema dotato di access point multipli e a una piattaforma di gestione centralizzata. Queste soluzioni sfruttano i singoli access point come semplici interfacce radio demandando il management a un dispositivo centrale. I vantaggi di una gestione centralizzata sono innanzitutto relativi alla sicurezza: l'intera struttura wireless risponde a dei criteri unificati, per cui all'aggiunta di un nuovo punto di accesso questo eredita automaticamente i parametri di protezione già impostati. La rete è inoltre in grado di individuare i cosiddetti *rogue AP*, punti di accesso che tentano di collegarsi alla rete senza la supervisione del sistema.

Dal punto di vista della mobilità, poi, la gestione centralizzata consente di attivare meccanismi di roaming in modo che un terminale possa passare dalla zona di copertura di un access point ad un altro in modo trasparente e senza la necessità di ri-autenticarsi a ogni passaggio sulla rete.

Una delle problematiche che affliggono più spesso le reti senza fili sono le interferenze provenienti da altri apparati wireless che operano nelle medesime frequenze. Se la vostra zona è particolarmente "trafficata", potete optare per una rete Wi-Fi che supporti anche le frequenze intorno ai 5 GHz, meno afflitte dai fenomeni di interferenza. Per poter operare in questo ambito, anche gli apparati terminali devono chiaramente supportare i 5 GHz. Molti access point professionali integrano un doppio apparato radio che consente di operare contemporaneamente a 2,4 e 5 GHz.

TUTTI SULLA NUVOLA

I servizi cloud-based hanno un forte impatto sulla pianificazione, la configurazione e la gestione della rete aziendale. Quale che sia il vostro settore professionale, i processi aziendali basati sulla struttura informatica sono infatti destinati, se non ora in futuro, ad essere strettamente integrati con le piattaforme cloud.

In ambito di storage e backup, ad esempio, l'impiego di servizi cloud permette di aumentare l'affidabilità conservando una copia dei dati sensibili in remoto, al riparo da eventuali eventi "catastrofici" che compromettano l'intera rete locale. Lo storage online si tramuta spesso in vera e propria piattaforma di collaborazione, per lo scambio di file e cartelle tra i membri di un gruppo di lavoro. D'altro canto, è altrettanto importante disporre dei propri dati anche in locale, in modo da poter accedervi in caso di necessità anche quando la connessione Internet non dovesse essere disponibile. Per abbinare i vantaggi dello storage online e offline, una delle soluzioni più adatte alle Pmi è rappresentato dai Nas, di cui parleremo più diffusamente tra qualche pagina. Molti modelli supportano infatti uno o più servizi di storage cloud-based come Amazon S3 attraverso i quali producono una copia remota dei dati indicati dall'amministratore di rete e presenti sul Nas. In questo modo è possibile ottenere una copia de-localizzata dei dati più sensibili senza dover intervenire sulle singole workstation della rete.

Oltre allo storage, il cloud può ospitare diverse applicazioni sostituendo il server locale. L'esempio più lampante è quello della posta elettronica: utilizzare un servizio professionale basato sul cloud non solo permette di fare a meno del server di posta, ma semplifica la sincronizzazione delle caselle tra i diversi dispositivi di accesso, fissi e mobili. Anche le suite di produttività più tradizionali sono direttamente integrate con

il cloud: Microsoft e Google, ad esempio, permettono di salvare i file sulle relative piattaforme di storage online (Google Drive e OneDrive). Il cloud può anche fornire server completi, ovvero macchine virtuali che si possono affittare solo per il tempo necessario, con tariffe orarie. Questa applicazione della *Infrastructure As A Service* è ideale per le realtà con esigenze variabili nel tempo; si pensi ad esempio a uno studio grafico che debba eseguire dei rendering ad altissime prestazioni per un progetto: sono sufficienti poche ore di affitto di un server per completare il task con costi in proporzione irrisori. Servizi di questo tipo sono Amazon Ec2 e Google Compute Engine.

La diffusione di servizi come quelli appena citati si riflette direttamente sulla struttura e su i dispositivi della rete: molte realtà Pmi possono ad esempio accontentarsi di un Nas per le esigenze di server comuni, dal momento che sono sempre meno le installazioni che richiedono veri e propri server applicativi. Inoltre, oltre alla già citata attenzione sulle prestazioni di connettività verso Internet, il cloud obbliga l'amministratore a ridisegnare le policy di accesso verso l'esterno, per abilitare, con opportune precauzioni, la fruibilità dei contenuti del cloud a tutti gli operatori autorizzati.

Anche Office di Microsoft diventa Software As A Service e l'integrazione con il cloud è sempre più spinta.

Aziende di piccole e medie dimensioni	Grandi imprese
<p>Vedi anche: Contenuto di tutti i piani Office 365 ProPlus. Piani per gli istituti scolastici. Piani per gli enti pubblici. Piani per organizzazioni non profit. Office per la casa. Domande frequenti.</p> <p>Il prezzo non include l'IVA.</p>	
<p>Office 365 Small Business</p> <p>Netto non è possibile sottoscrivere i piani Small Business con Office 365 Standard Business.</p> <p>€ 4,10 utente/mese pagamento annuale di € 49,20</p> <p>Acquista ora</p> <p>O € 4,50 per utente/fatturazione mensile</p>	<p>Office 365 Small Business Premium</p> <p>€ 10,40 utente/mese pagamento annuale di € 124,80</p> <p>Acquista ora</p> <p>Versione di valutazione gratuita O € 12,80 per utente/fatturazione mensile</p>
<p>Office 365 Midsize Business</p> <p>€ 12,30 utente/mese impegno annuale</p> <p>Acquista ora</p> <p>Versione di valutazione gratuita</p>	
<p>Numero massimo di utenti</p> <p>25 utenti</p>	<p>25 utenti</p> <p>300</p>
<p>Applicazioni Office: addebiatamento a Office per un massimo di 5 PC/tablet per utente.</p>	<p>Versioni destinate al cloud</p>
<p>Posta elettronica ospitata: posta elettronica ospitata 3 caselle condivise, 50 GB di spazio di archiviazione per utente e possibilità di utilizzare il proprio nome di dominio.</p>	
<p>Conferenze Web, presenza e messaggistica istantanea: conferenze Web sul Web con le funzionalità di videoconferenza HD, condivisione dello schermo e messaggistica istantanea. Condivide la presenza, i messaggi istantanei e le chiamate audio con gli utenti di Skype.</p>	
<p>Condivisione file semplificata: con SkyDrive Pro ogni utente dispone di 25 GB di spazio di archiviazione personale accessibile ovunque e sincronizzabile con i PC. Il file possono essere facilmente condivisi internamente o esternamente, controllando chi è autorizzato a visualizzarli e modificarli.</p>	

Cinque tip

1 Storage ibrido
Il cloud può rivelarsi una soluzione vincente per le esigenze di storage di una piccola azienda. Se però desiderate avere sempre a disposizione una copia dei file, anche offline, potete approntare un sistema di sincronizzazione dal server centrale o Nas.

2 Il cloud sicuro
Verificate le credenziali di sicurezza dei servizi cloud a cui aderite. In particolare sono fondamentali la cifratura delle trasmissioni e la codifica dei file che risiedono online.

3 Software as a service
Cloud non significa solo storage: anche le applicazioni possono spostarsi sulla nuvola, a partire da quelle essenziali per un piccolo ufficio come suite office e posta elettronica. I vantaggi vanno dal pagamento sulla base dell'utilizzo agli aggiornamenti automatici, passando per il costo ridotto di gestione.

4 Non solo applicazioni
Oltre allo storage e alle applicazioni, potete spostare sul cloud anche i server: questo approccio non è utile solo per ridurre il costo di acquisto e manutenzione delle macchine, ma anche per chi necessita di server con potenze e capacità variabili nel tempo.

5 Collaborazione
Il cloud si presta nativamente ai servizi di collaborazione: calendari condivisi, wiki aziendali, messaggistica istantanea dedicata, accesso alle risorse da remoto per telelavoratori e sedi distaccate sono solo alcune delle potenziali applicazioni.

Cinque tip

1 Il Byod è inevitabile

Il paradigma del Bring Your Own Device (Byod) sta facendo breccia nelle realtà aziendali di tutte le dimensioni. È inutile contrastarlo, ma è altrettanto importante saperlo gestire. La rete deve quindi essere predisposta per l'accesso da dispositivi personali.

2 Mobile Device Management

Gestire dispositivi mobili è un'operazione che richiede piattaforme articolate. I cosiddetti servizi di Mobile Device Management comprendono tipicamente agenti software da installare sui terminali e sistemi di controllo centralizzati, anche sul cloud.

3 Segmentare la rete

A livello di infrastruttura, può essere utile differenziare l'accesso da parte dei computer residenti e quello da apparati mobili come smartphone e tablet. In questo modo i servizi e le applicazioni più sensibili restano più protette dalle minacce esterne.

4 Policy chiare per tutti

Al di là delle soluzioni tecniche, è opportuno definire delle policy pratiche per l'utilizzo dei terminali mobili da parte del personale. Tali policy devono essere "pubblicate" in modo chiaro per essere accessibili a tutti i dipendenti.

5 Formazione

Per il personale abituato a operare su personal computer, l'approccio al mondo mobile può essere traumatico. Se decidete di integrare smartphone e tablet all'interno della vostra struttura informatica, dedicate le opportune risorse alla formazione del personale.

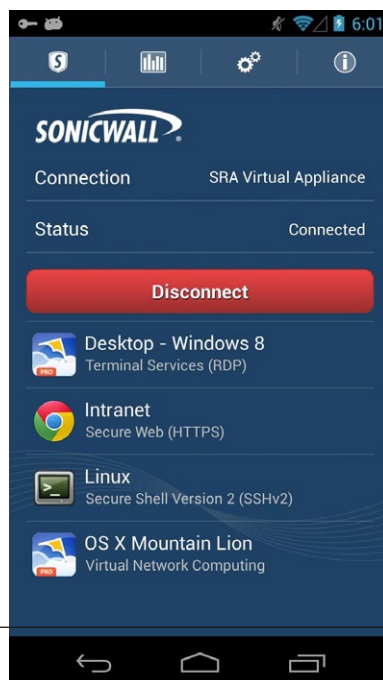
I DISPOSITIVI MOBILI

Nella progettazione di una moderna rete informatica non si può fare a meno di considerare l'accesso da parte di dispositivi mobili come smartphone e tablet. Come abbiamo già visto, questi apparati obbligano innanzitutto a predisporre una struttura Wi-Fi adeguata, ma non solo: una delle più importanti decisioni dell'amministratore riguarda la proprietà dei suddetti dispositivi. Un'opzione è quella di fornire gli apparati ai dipendenti, l'altra è quella di consentire l'utilizzo di terminali di proprietà del personale, secondo il paradigma, sempre più in voga, del *Bring Your Own Device* (Byod). I dispositivi mobili rappresentano una sfida impegnativa per l'amministratore di rete, innanzitutto poiché costituiscono una potenziale falla alla sicurezza: se infettati da malware possono infatti introdurre codice maligno all'interno dell'azienda, o esporre dati sensibili in essi conservati quando l'utente si collega a una rete wireless non sicura. Ancora, in caso di smarrimento o furto dell'apparato tutti i dati in esso conservati sono potenzialmente a rischio, se non si provvede a opportuna cifratura.

La gestione dei dispositivi mobili, e in particolare di quelli di proprietà del personale, può essere affrontata in diversi modi: il più radicale è quello di escludere totalmente tali apparati

dalla rete aziendale. Si tratta di una scelta miope in quanto ci si priva volontariamente di strumenti in grado di aumentare la produttività e la versatilità della struttura informatica nel suo complesso. Una seconda opzione è quella di limitare l'accesso a Internet, impedendo le comunicazioni verso i server aziendali, ad esempio approntando una rete wireless dedicata ai dispositivi mobili. In questo caso si proteggono i dati più sensibili, ma anche l'accesso a semplici applicazioni cloud-based, posta elettronica aziendale su tutti, mette a repentaglio la riservatezza dei dati.

La soluzione più efficiente è costituita dalle piattaforme di *Mobile Device Management*: sempre più diffusi sul mercato, questi sistemi si basano tipicamente su un software o servizio di controllo centrale dei dispositivi da un lato, e su un agente software da installare sui terminali dall'altro. Il sistema di gestione centrale permette all'amministratore di definire le policy da attuare sui dispositivi, incluse le metodologie di accesso alle risorse, oltre che di stabilire un canale di accesso sicuro. Gli agenti sui terminali verificano innanzitutto la "compliance" dei dispositivi: per poter accedere alle risorse aziendali, smartphone e tablet devono ad esempio essere dotati dell'ultimo sistema operativo supportato, non essere stati sottoposti a jailbreak o root, o ancora non aver installato software non autorizzato. L'agente può anche inibire l'accesso ai dati quando ci si collega a Internet tramite una rete Wi-Fi non autorizzata, o lo scambio di dati tra le applicazioni aziendali e quelle per uso personale. Le funzioni anti-malware contrastano l'installazione di codice maligno sul terminale, mentre i sistemi più avanzati sono dotati di un vero e proprio marketplace interno da cui installare le sole applicazioni verificate. Tra le piattaforme Mdm più diffuse, ricordiamo AirWatch e MobileIron, oltre agli storici Citrix, IBM, Sap e Symantec.



Sonicwall Secure Mobile Access: la nuova soluzione proposta da Dell per la gestione degli accessi alla rete da dispositivi mobili.

Un Nas per la piccola e media azienda deve supportare almeno quattro dischi rigidi.



NAS, NON SOLO STORAGE

I lettori di *PC Professionale* sanno bene quali siano i benefici che un Nas può apportare a una rete di piccole e medie dimensioni. I Network Attached Storage sono ormai di fatto dei veri e propri server di uso generico, che forniscono non solo spazio di storage condiviso, ma tutta una serie di applicazioni base che possono essere facilmente implementate anche dalle aziende con personale e competenze It ridotte. Abbiamo già accennato a come la diffusione dei servizi cloud abbia poi reso inutile per molte Pmi l'installazione in loco di server applicativi dedicati, e questo fenomeno rende i Nas ancora più attrattivi.

Nella scelta di un Nas concorrono diversi fattori, il cui peso varia in base alle esigenze specifiche: il numero di dischi supportati influenza direttamente la capacità massima gestibile dall'apparato, ma anche le prestazioni e il livello di affidabilità dei dati: più hard disk possono essere infatti configurati secondo architetture Raid che replicano i dati in modo da poter sopportare il guasto di una o più unità senza interruzione di servizio.

L'architettura più diffusa e indicata in ambito Pmi è il Raid 5, che richiede almeno tre dischi e può operare anche quando viene meno un singolo modulo. Un quarto disco può essere sfruttato come dispositivo di *hot spare* (ricambio a caldo) in modo da subentrare automaticamente in caso di guasto. Con quattro o più dischi si possono definire architetture anche più complesse, ma in ambito di piccolo e medio ufficio il nostro consiglio è quello di considerare i Nas a quattro baie, salvo esigenze particolari.

Altro elemento da tenere in particolare considerazione sono le interfacce di connessione presenti sul Nas. Queste si dividono essenzialmente in porte di rete e di espansione. Le prime sono sfruttate per collegare il Nas al network e sono tipicamente Gigabit Ethernet; molti Nas professionali dispongono di due porte Gigabit, al cui banda può essere aggregata per raggiungere la soglia massima nominale di 2.000 megabit al secondo. Se volete sfruttare questa caratteristica, verificate che lo switch di rete supporti l'aggregazione di banda sulle porte. Per esigenze prestazionali ancora superiori, i Nas più evoluti possono gestire anche porte a 10 Gigabit. Le porte di espansione (eSata e Usb) sono utilizzate invece per collegare al Nas dischi esterni. In ambito aziendale, questi sono tipicamente impiegati per conservare una copia di backup dei dati più sensibili presenti sul Nas, come ulteriore garanzia di affidabilità.

Sul fronte applicativo, i servizi imprescindibili che un Nas deve offrire sono un sistema di accesso versatile, con gestione di utenti e gruppi di lavoro, e compatibilità con tutti i protocolli di rete richiesti dalla vostra struttura informatica. I protocolli Smb, Nfs e Afp sono ormai supportati dalla quasi totalità dei Nas, consentendo un accesso completo alle risorse da parte di sistemi Windows, Mac e Linux.

Altrettanto importanti sono le funzioni di backup delle workstation: i Nas sono spesso forniti con software proprietari da installare sui Pc della rete, in alcuni casi gratuiti in altri sottoposti a licenza. È comunque possibile acquistare software di terze parti che supportino il backup in rete.

Cinque tip

1 Dischi e capacità
Il numero di dischi supportati dal Nas non influenza solo la capacità di storage complessiva, ma anche le modalità di configurazione dei moduli e gli standard di prestazioni e affidabilità. Per un utilizzo professionale, servono almeno 4 dischi.

2 Interfacce
Non prestate attenzione solo alle interfacce di rete (almeno due Gigabit, aggregabili), ma anche a quelle per l'aggancio di dischi esterni utili al backup del Nas. Le Usb 3.0 offrono le massime prestazioni, insieme alle porte eSata.

3 iScsi
Il protocollo iScsi consente di sfruttare il Nas anche come dispositivo Das (Directly Attached Storage). In questo modo può essere visto da un server preesistente come hard disk Scsi e quindi gestito come un normale modulo interno.

4 Backup e cloud
Il Nas deve poter gestire al meglio sia il backup delle macchine in rete sia quello dei suoi stessi dati verso moduli esterni. Per garantire ulteriore affidabilità, anche in ambito delocalizzato, può essere utile il supporto per la sincronizzazione con servizi di storage cloud-based.

5 Applicazioni per tutti
I Nas moderni non gestiscono solo lo storage ma possono trasformarsi in veri e propri application server gestendo siti Web dinamici, posta elettronica, Intranet e sistemi di videosorveglianza.

Cinque tip

1 Gruppi di continuità
Cali, sbalzi e interruzioni di corrente possono mettere a repentaglio gli apparati: investite quindi in opportuni gruppi di continuità per garantire l'alimentazione agli elementi chiave, come server, workstation e dispositivi di rete attivi strategici.

2 Ridondanza
Replicate le strutture cruciali in modo da mettervi al riparo da interruzioni di servizio: i Nas, ad esempio, possono essere configurati in modo da sincronizzare il modulo in servizio con una copia esatta che subentra in fail-over.

3 Parti di ricambio
In caso di guasto sulla componentistica, è bene disporre da subito di pezzi di ricambio da installare senza dover attendere i tempi di evasione di un ordine fornitori. Le parti più sensibili in questo senso sono dischi rigidi e alimentatori.

4 Reportistica e alert
Prevenire è meglio che curare: approntate un sistema di monitoraggio dei sistemi, con report periodici che informino l'amministratore di rete sullo stato dei dischi, le temperature di esercizio ed altre problematiche che possono interessare server e workstation aziendali.

5 Aggiornamenti hardware
Nas che operano in modalità degradata, dischi ancora operanti ma che segnalano problemi di vario genere, Pc che manifestano arresti anomali ricorrenti: non rimandate la sostituzione delle parti danneggiate.

AFFIDABILITÀ

I dati sensibili di una rete aziendale devono essere protetti non solo dalle minacce informatiche o da potenziali accessi che violino la riservatezza delle informazioni, ma anche dai guasti e dai malfunzionamenti che rischiano di corrompere i supporti e le strutture e quindi rendere file e servizi inutilizzabili.

Il problema dell'affidabilità copre scenari di vario genere, a partire dalle problematiche relative all'impianto elettrico per passare ai guasti dovuti alla naturale usura delle componenti, sino a toccare gli eventi causati da imperizia del personale.

I gruppi di continuità permettono di far fronte a interruzioni di corrente elettrica mantenendo attivi i dispositivi più strategici per il business. I modelli che offrono autonomia estesa sono molto costosi, ma spesso è sufficiente garantire al personale il tempo per salvare in modo sicuro i dati su cui si sta lavorando prima che avvenga uno spegnimento non controllato dei computer. In questo senso è fondamentale che il gruppo di continuità alimenti i server con le informazioni più strategiche; molti Nas possono interagire automaticamente con il gruppo di continuità, effettuando un arresto sicuro quando si rileva una interruzione sulla linea elettrica principale. I gruppi di continuità mettono inoltre i dispositivi al riparo da balzi di tensione che possono danneggiare le parti elettriche e possono proteggere anche la linea telefonica.

In caso di guasti sugli apparati, è possibile evitare interruzioni di servizio introducendo nella rete elementi ridondanti: il Nas può ad esempio essere

uplicato su una seconda macchina che subentra automaticamente in caso di problemi al modulo principale. La ridondanza può essere implementata anche all'interno dei singoli apparati. Server e switch professionali, ad esempio, spesso integrano gruppi di alimentazione doppi in modo da mantenere la propria attività in caso di guasto sulla singola unità.

I Nas sono uno degli esempi più lampanti di ridondanza: oltre alle già citate architetture Raid sui dischi, offrono spesso alimentatori multipli, doppie memorie flash per il caricamento del sistema operativo e interfacce di rete ridondanti.

Un amministratore di rete previdente non aspetta che il problema si verifichi per intervenire, ma previene la situazione critica, dotandosi ad esempio di tutte le parti di ricambio necessarie. Buona norma è ad esempio quella di conservare qualche disco vergine da utilizzare in caso di guasto sul Nas o su una workstation.

Discorso analogo vale per le memorie. Altra forma di prevenzione è l'aggiornamento dei sistemi: mantenere nel parco macchine componentistica obsoleta espone la struttura informatica a rischi sempre crescenti.

A volte è bene non indugiare troppo nella sostituzione dei pezzi, anche a costo di investire parte del budget per gli aggiornamenti.

Alla base di queste considerazioni deve esserci un efficiente sistema di monitoraggio e notifica: fortunatamente i dispositivi informatici più moderni integrano nativamente strumenti di controllo e prevenzione dei guasti.



Molti server professionali possono montare un doppio alimentatore per massimizzare l'affidabilità.